

Jhu



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,121	08/15/2001	Toyoaki Kishimoto	212668US6	1335

22850 7590 03/09/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER

TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 03/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

This action is in response to the Application filed on August 15, 2001.

5 Claims 1-12 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

10 (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15

Claims 1-6, and 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US Patent 5,708,780) further in view of Ericsson.

20 Regarding Claim 1, Levergood et al. teaches a user authentication method for an authentication server which executes user authentication between a [client] and a content providing server interconnected by an open network not guaranteeing the security of data to be transferred, comprising the steps of:

25 registering unique identification information stored in said [client] with a customer database of said authentication server in advance (see col.3 lines 21-43 reference "SID" for "unique identification information");

decoding the unique identification information encrypted by a predetermined encryption algorithm and supplied from said [client] terminal via said open network (see col.3 lines 34-37 reference "encrypted with a secret key");

5 determining whether the unique identification information decoded in the decoding step is registered with said customer database (see col.3 lines 43-48 reference "validate the SID"); and

10 sending a notification to said content providing server that starting of service provision for said [client] be permitted, if the unique identification information is found registered with said customer database in the determining step (see col.3 lines 43-48 reference ""content server receives a URL request accompanied by an SID").

Levergood et al. fails to teach the abovementioned system wherein the client is a "mobile information terminal".

15 Ericsson teaches the important of "enabling users of PCs connection to the Internet via mobile telephones, handheld devices, and smartphones to download Web pages more quickly" (see Ericsson).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Levergood et al. the wireless capabilities as described in Ericsson to provide for users connected to the Internet via mobile information terminals or handheld devices.

Regarding Claim 2, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to Claim 1, further comprising the step of:

presenting, to said mobile information terminal, a recommended menu including
5 site access information for accessing a plurality of predetermined content providing servers (see Levergood et al. col.8 lines 27-58 reference ""customize user requested pages to include personalized content");

wherein a process in which site access information selected by a user of said mobile information terminal from said recommended menu displayed on said mobile
10 information terminal is registered with said customer database in relation with the unique identification information of said mobile information terminal is included in the registering step (see Levergood et al. col.4 lines 32-42).

Regarding Claim 3, the combined method of Levergood et al. and Ericsson
15 teaches the user authentication method according to Claim 2, wherein, in the registering step, when registering said site access information with said customer database, user authentication is performed on the basis of said unique identification information before this registration and said mobile information terminal requested to make display for prompting said user to enter a password of the user (see Levergood et al. col.6 lines 44-
20 49 reference "causes the client browser to prompt the user for credentials, a preferred credential query typically consists of a request for user name and password"), while, subsequent to the registration with said customer database, an access request is made

Art Unit: 2137

on the basis of the site access information already registered with said customer database, the user authentication on the basis of said unique identification information is performed but the request for the display for prompting the user to enter the user's password is omitted (see Levergood et al. col.6 lines 40-44 reference "forgo the
5 credential check procedures").

Regarding Claim 4, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to Claim 3, wherein, in the registering step, a charging server is instructed to charge said user for the use of a service
10 provided by said content providing server associated with said site access information at the time of registering said site access information with said customer database (see Levergood et al. col.9 lines 1-6 reference "a user may be charged and billed each time she accesses a particular document through the internet").

15 Regarding Claim 5, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to Claim 4, wherein, in the registering step, a confirmation step for confirming, before instructing said charging server for the charging, that said user is a registered user of said charging server is included (see
Levergood et al. col.9 lines 1-6).

20 Regarding Claim 6, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to claim 1, wherein said open

network is the Internet, through which the unique identification information is transmitted as encrypted by the predetermined encryption algorithm by a Web browser installed on said mobile information terminal (see Levergood et al. col.3 lines 8-23).

5 Regarding Claim 9, Levergood et al. teaches a user authentication server which executes user authentication between a [client] and a content providing server interconnected by an open network not guaranteeing the security of data to be transferred, comprising:

 registering means for registering unique identification information stored in said
10 [client] with a customer database of said authentication server in advance (see col.3 lines 21-43 reference "SID" for "unique identification information");

 decoding means for identification information decoding the unique encrypted by a predetermined encryption algorithm and supplied from said [client] via said open network (see col.3 lines 34-37 reference "encrypted with a secret key");

15 determining means for determining whether the unique identification information decoded by the decoding means is registered with said customer database (see col.3 lines 43-48 reference "validate the SID"); and

 service permission notice sending means for sending a notification to said
content providing server that starting of service provision for said [client] be permitted,
20 the unique identification information is found registered with said customer database by the determining means (see col.3 lines 43-48 reference ""content server receives a URL request accompanied by an SID").

Levergood et al. fails to teach the abovementioned system wherein the client is a "mobile information terminal".

Ericsson teaches the important of "enabling users of PCs connection to the Internet via mobile telephones, handheld devices, and smartphones to download Web pages more quickly" (see Ericsson).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Levergood et al. the wireless capabilities as described in Ericsson to provide for users connected to the Internet via mobile information terminals or handheld devices.

10

Regarding Claim 10, teaches the user authentication server according to Claim 9, wherein said open network is the Internet, through which the unique identification information is transmitted as encrypted by the predetermined encryption algorithm by a Web browser installed on said mobile information terminal (see Levergood et al. col.3 lines 8-23).

15

Claims 7, 8, 11, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US Patent 5,708,780) and Ericsson as applied to Claims 1-6 and 9-10 above, and further in view of Wan (US Patent 6,044,069).

20

Regarding Claim 7, the combined method of Levergood et al. and Ericsson teaches the user authentication method according to Claim 6, wherein unique

Art Unit: 2137

identification information is read, by said Web browser, from said mobile information terminal and the retrieved unique identification information is transmitted as encrypted by the predetermined encryption algorithm by said Web browser.

Levergood et al. and Ericsson fails to teach the abovementioned method wherein
5 the unique identification information is read from a flash memory installed on said mobile information terminal.

Wan teaches the use of flash memory in mobile information terminals for the purpose of storing non-volatile information (see Wan reference "mobile station identifier" and "flash").

10 It would have been obvious to a person of average skill in the area at the time of the invention to include within Levergood et al. and Ericsson the flash storage and retrieval of information as described in Wan to provide users with memory that is quieter, faster, smaller, lighter, and non-volatile.

15 Regarding Claim 8, the combined method of Levergood et al., Ericsson, and Wan teaches the user authentication method according to Claim 7, wherein said predetermined encryption algorithm is SSL (Secure Socket Layer) (see Ericsson reference "Netscape Navigator" and "Microsoft Internet Explorer" both of which utilize a version of SSL, and "WAP" which utilizes TSL, a version of SSL).

20

Regarding Claim 11, the combined method of Levergood et al. and Ericsson teaches the user authentication server according to claim 10 wherein unique

identification information is read, by said Web browser from said mobile information terminal and the retrieved unique identification information is transmitted as encrypted by the predetermined encryption algorithm by said Web browser (see Wan).

Levergood et al. and Ericsson fails to teach the abovementioned method wherein
5 the unique identification information is read from a flash memory installed on said mobile information terminal.

Wan teaches the use of flash memory in mobile information terminals for the purpose of storing non-volatile information (see Wan reference "mobile station identifier" and "flash").

10 It would have been obvious to a person of average skill in the area at the time of the invention to include within Levergood et al. and Ericsson the flash storage and retrieval of information as described in Wan to provide users with memory that is quieter, faster, smaller, lighter, and non-volatile.

15 Regarding Claim 12, the combined method of Levergood et al., Ericsson, and Wan teaches the user authentication server according to claim 11 wherein said predetermined encryption algorithm is SSL (see Ericsson reference "Netscape Navigator" and "Microsoft Internet Explorer" both of which utilize a version of SSL, and "WAP" which utilizes TSL, a version of SSL).

Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

20 
Tamara Teslovich
March 4, 2005